ABSTRACT OF THE DISCLOSURE

[56] The security of block cipher counter mode of operation can be improved, and stream ciphers can be converted to a "block-like" (stateless) mode of operation, by using a modified key which is a fixed secret key (K) combined with a varying random non-secret byte sequence (J) with same size as the keysize of key K. In accordance with various embodiments, the modified key can be generated by XORing the fixed secret key with a varying random sequence that is newly generated for each plaintext message. Alternatively, the fixed secret key can be modified with a variable, non-secret initialization vector and used with stream ciphers. In still another embodiment, the key and sequence are concatenated and passed through a mask generation function.